QUADRATIC FORMS REPRESENTING THE pTH FIBONACCI NUMBER

PEDRO BERRIZBEITIA, FLORIAN LUCA, AND ALBERTO MENDOZA

ABSTRACT. In this paper, we show that if $p \equiv 1 \pmod 4$ is prime, then $4F_p$ admits a representation of the form $u^2 - pv^2$ for some integers u and v, where F_n is the nth Fibonacci number. We prove a similar result when $p \equiv -1 \pmod 4$.

Keywords and phrases. Fibonacci numbers, norms of algebraic numbers, Galois theory.

2010 Mathematics Subject Classification. 11B39.

1. Introduction

Let $\{F_n\}_{n\geq 0}$ be the Fibonacci sequence given by $F_0 = 0,\ F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. The starting point for the investigation of the subject in the title is the formula

$$F_{2n+1} = F_n^2 + F_{n+1}^2 \tag{1}$$

known to Lucas (take $Q = -1$ in formula (34) in Lucas's seminal 1878 paper [4]) since it implies that every Fibonacci number of odd index can be represented as the sum of two squares of integers numbers. This is a question which leads naturally to the investigation of Fibonacci numbers F_n which can be represented under the form $u^2 + dv^2$ with some integers u and v and some integer d which is either fixed or depends on n. For example, in [6], it is shown that if $n \equiv 7 \pmod{16}$, then $F_n = u^2 + 9v^2$ holds with some positive integers u and v. For general results regarding this problem when d is fixed, see [3].

In [2], it was noted that if $n = p^2$ is the square of an odd prime $p \neq 5$, then p divides $F_{\frac{p^2-1}{2}}$, hence formula (1) implies that $F_{p^2} = u^2 + p^2v^2$, for some integers u and v. Motivated by this observation, they introduced and estimated the counting function of the infinite set

$$S = \{n\ :\ F_n = u^2 + nv^2 \text{ with some integers } u, v\}.$$

In the course of their investigation, they found computational evidence that indicated that every prime $p \equiv 1 \pmod 4$ belongs to S. In [1], it was proved this fact is true; that is that if $p \equiv 1 \pmod 4$, then $F_p = u^2 + pv^2$ for some integers u and v. The proof makes use of

Date: February 17, 2015.

basic facts in Galois Theory and basic properties of the norm function of finite extensions of $\mathbb{Q}$. Prior, it was shown in [6] that the above formula never holds if instead of $p \equiv 1 \pmod 4$, we have $p \equiv 3, 7 \pmod{20}$. In this paper, we find quadratic forms representing F_p, for all primes $p \equiv -1 \pmod 4$. In fact, we extend the method developed in [1] to study other quadratic form representations for F_p or $4F_p$, all depending only on the congruence modulo 4 of the prime p. We state the main result of this paper:

Theorem 1. (i) *If $p \equiv 1 \pmod 4$ is prime, then $4F_p = u^2 - pv^2$ holds with some (in fact, infinitely many) pairs of positive integers (u, v).*
(ii) *If $p \equiv -1 \pmod 4$, then $4F_p = 5u^2 + pv^2$ holds with some integers u and v.*

2. The proof of Theorem 1

For a positive integer n let ζ_n be a primitive nth root of unity. We let

$$(\alpha, \beta) = ((1 + \sqrt{5})/2, (1 - \sqrt{5})/2),$$

and use the fact that

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{holds for all} \quad n \geq 0. \tag{2}$$

Our proof proceeds by noting that formula (2) entails

$$F_n = \prod_{t=1}^{n-1} (\alpha - \beta \zeta_n^t). \tag{3}$$

We assume that $n = p$ is an odd prime and denote the field $\mathbb{Q}(\sqrt{5}, \zeta_p)$ by $\mathbb{L}$. We let $p^* = (-1)^{\frac{p-1}{2}} p$. For any subfield $\mathbb{F}$ of $\mathbb{L}$, and for any $\gamma \in \mathbb{L}$, $N_{\mathbb{L}/\mathbb{F}}(\delta)$ will denote the relative norm of γ from $\mathbb{L}$ to $\mathbb{F}$. So $N_{\mathbb{L}/\mathbb{F}}(\gamma) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{F})} \sigma(\gamma)$, where $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is the Galois Group of $\mathbb{L}$ over $\mathbb{F}$.

Note that $\mathbb{L}$ is a number field of degree $2(p-1)$ over $\mathbb{Q}$, that is, $[\mathbb{L} : \mathbb{Q}] = 2(p-1)$.

Note further that $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = \langle \tau \rangle \times \langle \sigma_5 \rangle$, where

- $\tau(\zeta_p) = \zeta_p^g$ for some generator g of $\mathbb{Z}_p^*$, and $\tau(\sqrt{5}) = \sqrt{5}$;
- $\sigma_5(\zeta_p) = \zeta_p$, and $\sigma_5(\sqrt{5}) = -\sqrt{5}$.

For integers d and d' we let $\mathbb{Q}_d = \mathbb{Q}(\sqrt{d})$ and we let $\mathbb{Q}_{d,d'} = \mathbb{Q}(\sqrt{d}, \sqrt{d'})$. The following diagram of subfields of $\mathbb{L}$ is useful:

$$\begin{tikzcd}
& L=\mathbb{Q}(\sqrt{5},\zeta_p) \arrow[d, dash, "\tau^2"'] & \\
& K=\mathbb{Q}_{5,p^*} \arrow[dl, dash, "\tau"'] \arrow[d, dash, "\tau\sigma_5"] \arrow[dr, dash, "\sigma_5"] & \\
\mathbb{Q}_5 \arrow[dr, dash, "\sigma_5"] & \mathbb{Q}_{5p^*} \arrow[d, dash, "\tau=\sigma_{p^*}"] & \mathbb{Q}_{p^*} \arrow[dl, dash, "\tau"] \\
& \mathbb{Q} &
\end{tikzcd}$$

From the diagram, one can see that

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \langle \tau^2 \rangle,$$

$$\mathrm{Gal}(\mathbb{L}/\mathbb{Q}_5) = \langle \tau \rangle,$$

$$\mathrm{Gal}(\mathbb{L}/\mathbb{Q}_{p^*}) = \langle \tau^2 \rangle \times \langle \sigma_5 \rangle,$$

$$\mathrm{Gal}(\mathbb{L}/(\mathbb{Q}_{5p^*}) = \langle \tau\sigma_5 \rangle.$$

From (2), we obtain

$$F_p = \prod_{t=1}^{p-1}(\alpha - \beta\zeta_p^t) = \prod_{s=1}^{p-1}(\alpha - \beta\tau^s(\zeta_p)) = N_{\mathbb{L}/\mathbb{Q}_5}(\alpha - \zeta_p\beta).$$

We let $\gamma = \alpha - \zeta_p\beta$, so $\gamma \in \mathbb{L}$. We also let

$$\Gamma = N_{\mathbb{L}/\mathbb{K}}(\gamma) = \prod_{t=1}^{\frac{p-1}{2}}(\alpha - \tau^{2t}(\zeta_p)\beta) = \prod_{r\in R}(\alpha - \zeta^r\beta),$$

where R is the set of quadratic residues in $\mathbb{Z}_p^*$. Again from (2), we get

$$F_p = \prod_{t=1}^{p-1}(\alpha - \zeta_p^t\beta) = \prod_{r\in R}(\alpha - \zeta_p^r\beta)\prod_{r\in R}(\alpha - \zeta_p^{gr}\beta),$$

where $\tau(\zeta_p) = \zeta_p^g$. It follows that $F_p = \Gamma\tau(\Gamma)$. Next we compute $\sigma_5(\Gamma)$ and get:

$$\sigma_5(\Gamma) = \prod_{r\in R} \sigma_5(\alpha - \zeta_p^r\beta) = \prod_{r\in R} (\beta - \zeta_p^r\alpha) = \prod_{r\in R} \left(\frac{-1}{\alpha} + \frac{1}{\zeta_p^{-r}\beta}\right) = \frac{\prod_{r\in R}(\alpha - \zeta_p^{-r}\beta)}{(-1)^{\frac{p-1}{2}}\prod_{r\in R}\zeta_p^r},$$

where we have used for the last three equalities that

$$\sigma_5(\alpha) = \beta, \quad \sigma_5(\beta) = \alpha, \quad \sigma_5(\zeta_p) = \zeta_p \quad \alpha\beta = -1,$$

which are all trivial to verify. This leads to the following:

(1) if $p \equiv 1 \pmod 4$ then $\sigma_5(\Gamma) = \Gamma$;
(2) if $p \equiv -1 \pmod 4$ then $\sigma_5(\Gamma) = -\tau(\Gamma)$.

2.1. **Case i) of Theorem 1.** In that case $\sigma_5(\Gamma) = \Gamma$, so Γ is fixed by τ^2 and by σ_5. It follows that $\Gamma \in \mathbb{Q}_{p^*}$. Hence, $\Gamma = x + y\sqrt{p}$ for some half integers x and y. Since $F_p = \Gamma\tau(\Gamma)$, then $F_p = x^2 - py^2$. Multiplying Γ by norm 1 units of the ring of integers of $\mathbb{Q}_p$ leads to infinitely many solutions.

2.2. **Case ii) of Theorem 1.** Now $p^* = -p$ and $\sigma_5(\Gamma) = -\tau(\Gamma)$. Since we have $\Gamma \in K = \mathbb{Q}_{5,-p}$, we get that

$$\Gamma = r + s\sqrt{5} + t\sqrt{-p} + u\sqrt{-5p} \tag{4}$$

with rational numbers r, s, t, u whose denominator divides 4. The condition

$$\sigma_5(\Gamma) = -\tau(\Gamma) \quad \text{implies} \qquad r = u = 0.$$

It follows that $\Gamma = s\sqrt{5} + t\sqrt{-p}$. Apriori, $4s$ and $4t$ are integers. We need to be more precise and justify that $2s$ and $2t$. In order to do so, we argue as follows. The quadratic fields $\mathbb{Q}_5$ and $\mathbb{Q}_{-p}$ have integral bases $\{1, (1+\sqrt{5})/2\}$, (respectively $\{1, (1+\sqrt{-p})/2\}$) and coprime discriminants 5 and $-p$. It follows that an integral basis for $\mathbb{Q}_{5,-p}$ is

$$\{1, (1+\sqrt{5})/2, (1+\sqrt{-p})/2, (1+\sqrt{5})(1+\sqrt{-p})/4\}$$

(see Exercise 4.5.13 in [5]). Hence, for some integers a, b, c, d, we have

$$\begin{aligned} \Gamma &= a + b(1+\sqrt{5})/2 + c(1+\sqrt{-p})/2 + d(1+\sqrt{5})(1+\sqrt{-p})/4 \\ &= (a + b/2 + c/2 + d/4) + (b/2 + d/4)\sqrt{5} + (c/2 + d/4)\sqrt{-p} + (d/4)\sqrt{-5p}. \end{aligned} \tag{5}$$

Identifying coefficients in (4) and (5), we get

$$r = a + b/2 + c/2 + d/4, \quad s = b/2 + d/4, \quad t = c/2 + d/4, \quad u = d/4.$$

Since $r = u = 0$, we get $d = 0$, therefore $2s = b$ and $2u = c$ are integers. Since $F_p = \Gamma\tau(\Gamma) = 5s^2 + pt^2$, we get the desired result.

References

[1] J. J. Alba González, P. Berrizbeitia and F. Luca, "On the formula $F_p = u^2 + pv^2$", *Internat. J. Number Theory* **11** (2015), 185–191.

[2] J. J. Alba González and F. Luca, "On the positive integers n satisfying the equation $F_n = x^2 + ny^2$", *Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms, Contemporary Mathematics*, Vol. 587 (American Mathematical Society, Providence, RI, 2013), pp. 95–109.

[3] C. Ballot and F. Luca, "On the equation $x^2 + dy^2 = F_n$", *Acta Arith.* **127** (2007), 145–155.

[4] E. Lucas, "Théorie des fonctions numériques simplement périodiques", *Amer. J. Math.* **1** (1878), 184–240, 289–321.

[5] M. R. Murty and J. Esmonde, *Problems in Algebraic Number Theory*, Second Edition, Springer 2004.

[6] D. Savin, "Fibonacci primes of special forms", *Notes on Number Theory and Discrete Math.* **20** (2014), 10–19.

Departamento de Matemáticas Pura y Aplicada, Universidad Simón Bolívar, Caracas, Venezuela

E-mail address: pberrizbeitia@gmail.com

School of Mathematics, University of the Witwatersrand, P. O. Wits 2050, South Africa

E-mail address: florian.luca@wits.ac.za

Departamento de Matemáticas Pura y Aplicada, Universidad Simón Bolívar, Caracas, Venezuela

E-mail address: jacob@usb.ve